**Rang d'un module libre de type fini.**
Soient $R$ un anneau commutatif et $F$ un $R$-module libre de type fini de base $\mathcal{B}$. Si $\mathcal{M}$ représente un idéal maximal de $R$, montrer que

a) Le $R$-module quotient $F/\mathcal{M}F$ est aussi un $R/\mathcal{M}$-espace vectoriel,

b) La famille $\left\{\dot{b}\right\}_{b\in\mathcal{B}}$ est une base de cet espace vectoriel.

En déduire que toutes les bases de $F$ ont le même nombre $r$ d'éléments (ce nombre est appelé rang, ou dimension, du module $F$). On a montré l'équivalence entre les affirmations suivantes concernant un $R$-module $F$ :

i) $F$ est un $R$-module libre de type fini,

ii) Il existe un unique entier naturel $r$ non nul tel que $F \simeq R^r = R \oplus R \oplus ... \oplus R$.

---

Solution :

a) $\mathcal{M}$ = idéal maximal $\Rightarrow$ $R/\mathcal{M}$ corps.

$\mathcal{M}F$ = sous-module de $F$ engendré par les produits $m\beta$ où $m \in \mathcal{M}$ et $\beta \in F$

$= \left\{ \sum_{\text{somme finie}} m_i \beta_i \;/\; m_i \in \mathcal{M} \text{ et } \beta_i \in F \right\}$

Pour vérifier que $F/\mathcal{M}F$ est un $R/\mathcal{M}$-espace vectoriel, il suffit de prouver que la loi externe naturelle

$$\forall\, \dot{\lambda} \in R/\mathcal{M} \quad \forall\, \dot{\beta} \in F/\mathcal{M}F \qquad \dot{\lambda}.\dot{\beta} = \dot{\overline{\lambda\beta}}$$

est bien définie. Cela provient de :

$$\left.\begin{array}{l} \lambda - \lambda' \in \mathcal{M} \\ \beta - \beta' \in \mathcal{M}F \end{array}\right\} \Rightarrow \lambda\beta - \lambda'\beta' = \underbrace{\lambda}_{\in R}\underbrace{(\beta-\beta')}_{\in \mathcal{M}F} + \underbrace{\beta'}_{\in F}\underbrace{(\lambda-\lambda')}_{\in \mathcal{M}} \in \mathcal{M}F .$$

b) $\{\dot{b}\}_{b\in\mathcal{B}}$ est clairement un système générateur de $F/\mathcal{M}F$. Montrons que c'est un système libre :

$$\sum_{b\in\mathcal{B}} \dot{\alpha}_b \dot{b} = \dot{0} \Rightarrow \sum_{b\in\mathcal{B}} \alpha_b b \in \mathcal{M}F \underset{(*)}{\Rightarrow} \sum_{b\in\mathcal{B}} \alpha_b b = \sum_{b\in\mathcal{B}} m_b b$$

($\mathcal{B}$ est une base du $R$-mod. $F$)

$$\Downarrow$$

$$\forall b \quad \alpha_b = m_b \in \mathcal{M}$$

$$\Downarrow$$

$$\forall b \in \mathcal{B} \quad \dot{\alpha}_b = \dot{0} \qquad \square$$

(*) en effet, $x \in \mathcal{M}F$ ssi $x$ s'écrit

$$x = \sum_i m_i \beta_i = \sum_i \underbrace{m_i}_{\in \mathcal{M}} \Big( \sum_{b\in\mathcal{B}} \underbrace{\beta_{b,i}}_{\in R} b \Big) = \sum_{b\in\mathcal{B}} m_b\, b. \quad \text{avec } m_b \in \mathcal{M}$$

[0] [umod0002] Dany-Jack Mercier, réf. BALCERZYK M. & JOSEFIAK T., "Commutative Rings", Ellis Horwood Series in Math. and it's applications, 1989, p31.

**Epimorphisme (resp. monomorphisme) direct.**

1) Soient $R$ un anneau commutatif et $f : M \to N$ un épimorphisme de $R$-modules. Montrer qu'il y a équivalence entre les deux propriétés suivantes :

i) Il existe un sous-module $H$ de $M$ tel que $M = \operatorname{Ker} f \oplus H$,

ii) Il existe un morphisme $g : N \to M$ tel que $f \circ g = Id_N$.

Dans ce cas, on dit que l'épimorphisme $f$ est direct.

2) Si $N$ est un $R$-module libre, montrer que tout épimorphisme $f : M \to N$ est direct.

3) On suppose maintenant que $f : M \to N$ un monomorphisme de $R$-modules. Montrer l'équivalence entre les propriétés suivantes :

i) Il existe un sous-module $H$ de $M$ tel que $N = \operatorname{Im} f \oplus H$,

ii) Il existe un morphisme $g : N \to M$ tel que $g \circ f = Id_M$.

Dans ce cas, on dit que le monomorphisme $f$ est direct.

---

Solution :

1) i) $\Rightarrow$ ii) : Posons

$$\begin{array}{rccc} g: & N & \to & M \\ & n & \mapsto & h \end{array}$$

où $h$ vérifie $n = f(a)$ et $a = k + h$ avec $k \in \operatorname{Ker} f$ et $h \in H$.

- L'application $g$ est bien définie puisque

$$\left\{ \begin{array}{l} n = f(a) = f(b) \\ a = k + h \\ b = k' + h' \end{array} \right. \Rightarrow f(h) = f(h') \Rightarrow h - h' \in \operatorname{Ker} f \cap H = \{0\} \Rightarrow h = h'.$$

- L'application $g$ est clairement linéaire.

- Pour tout $n \in N$, $f \circ g(n) = f(h) = f(a) = n$ donc $f \circ g = Id_N$.

ii) $\Rightarrow$ i) : Montrons que $M = \operatorname{Ker} f \oplus \operatorname{Im} g$.

-

$$m \in \operatorname{Ker} f \cap \operatorname{Im} g \Rightarrow f(m) = 0 \text{ et } m = g(n) \text{ avec } n \in N \Rightarrow n = f \circ g(n) = 0 \Rightarrow m = 0.$$

- Si $m = k + g(n)$ avec $k \in K$, alors $f(m) = f \circ g(n) = n$. Si la décomposition existe, ce sera

$$m = (m - g \circ f(m)) + g \circ f(m).$$

Réciproquement, il est facile de vérifier que cette décomposition convient, autrement dit que $m - g \circ f(m) \in \operatorname{Ker} f$ et $g \circ f(m) \in \operatorname{Im} g$.

2) Par hypothèse, le module $N$ possède une base $\{e_i\}_{i \in I}$. L'application $f$ est surjective donc

$$\forall i \in I \quad \exists m_i \in M \quad f(m_i) = e_i.$$

Il suffit de définir le morphisme $g : N \to M$ sur la base $\{e_i\}_{i \in I}$ en posant $g(e_i) = m_i$ pour obtenir $f \circ g = Id_N$.

---

[0] [umod0003] Dany-Jack Mercier réf. NORTHCOTT D.G., An introduction to homological algebra, Cambridge Univ. Press, 1960, Proposition 1 p12.

3) i) $\Rightarrow$ ii) : Posons

$$\begin{array}{rccc} g: & N & \to & M \\ & n & \mapsto & m \end{array}$$

où $m$ vérifie $n = f(m) + h$ avec $k \in H$.

- L'application $g$ est bien définie puisque

$$n = f(m) + h = f(m') + h' \Rightarrow f(m - m') = h' - h \in \operatorname{Im} f \cap H\{0\} \Rightarrow h = h'$$

d'où $f(m) = f(m')$ et $m = m'$ puisque $f$ est injective.

- L'application $g$ est clairement linéaire.
- Pour tout $m \in M$, on a $g \circ f(m) = m$ par définition.

ii) $\Rightarrow$ i) : Montrons que $N = \operatorname{Im} f \oplus \operatorname{Ker} g$.

- 

$$x \in \operatorname{Im} f \cap \operatorname{Ker} g \Rightarrow \exists m \in M \quad x = f(m) \text{ et } g(x) = 0 \Rightarrow g \circ f(m) = 0 \Rightarrow m = 0 \Rightarrow x = 0.$$

- Si $n \in N$ s'écrit $n = f(m) + k$ avec $k \in \operatorname{Ker} g$, alors $g(n) = m$ et la décomposition ne peut être que

$$n = f \circ g(n) + (n - f \circ g(n)).$$

Réciproquement, on peut vérifier que cette décomposition convient.